

APT28 hijacks DNS settings on vulnerable routers to steal credentials



The UK NCSC reports that APT28 has exploited vulnerable routers to change DHCP/DNS settings and run adversary-in-the-middle attacks that harvest passwords and OAuth tokens, including against Outlook-related domains.

- APT28 overwrote DHCP/DNS settings on compromised routers so traffic was resolved by attacker-controlled DNS servers.
- Resulting adversary-in-the-middle attacks aimed to harvest passwords and OAuth tokens for web and email services.
- One exploited model was the TP-Link WR841N, likely via CVE-2023-50224; many other TP-Link models were also targeted.
- Activity since 2024 into 2026 appears opportunistic, with victims filtered later for intelligence

value.

- Targeted domains included several Outlook-related names; the NCSC advises holistic detection because specific indicators change.

The UK National Cyber Security Centre (NCSC) has published details of how the Russian actor APT28 abuses routers to hijack DNS. The NCSC assesses the group is almost certainly GRU Military Intelligence Unit 26165.

What the actor is doing

APT28 exploits vulnerable routers, mainly small office/home office devices, and rewrites their DHCP DNS settings to point at actor-owned servers. Downstream devices such as laptops and phones inherit those settings. Lookups for domains tied to email or login pages are resolved to attacker infrastructure, while other requests go to legitimate addresses, which helps the activity stay quiet.

The actor then attempts adversary-in-the-middle attacks against follow-on connections, in browsers and desktop applications, to capture passwords and OAuth or similar tokens. The NCSC believes the campaign is opportunistic: a wide pool of users is observed first, then filtered for likely intelligence value.

One exploited model was the TP-Link WR841N, likely through CVE-2023-50224, which lets an unauthenticated attacker obtain credentials through crafted HTTP GET requests. A second request then changes the DNS settings. The advisory lists many further TP-Link models, and a second infrastructure cluster involved MikroTik and TP-Link routers.

Why it matters

Routers at branch offices, remote staff homes or small sites can silently redirect authentication traffic, exposing credentials for email and web services. The NCSC notes that specific indicators are liable to change, so detection should rely on broader tradecraft rather than only on IP lists.

NCSC mitigations include never exposing management interfaces to the internet, keeping devices and networks up to date with prompt security updates, and using modern systems and software.

What to do now

1. Inventory routers at branches, remote-work sites and small offices, and identify TP-Link and MikroTik models, including those listed by the NCSC.
2. Verify the DHCP/DNS settings on these devices against approved resolvers and investigate any unknown DNS server addresses.
3. Ensure router management interfaces are never reachable from the internet, and apply the latest vendor security updates, including for CVE-2023-50224.
4. Monitor DNS and sign-in logs for unusual resolutions of email and login domains and for logins from

unexpected infrastructure.

5. Review OAuth tokens and sessions for potentially exposed accounts, and reset credentials where DNS tampering is found.